SDN COMMUNICATIONS.

JAN. - JUNE 2019

CYBER THREAT LANDSCAPE

Cybersecurity Intelligence Report

EXECUTIVE SUMMARY

This report contains observations and insights from our SDN Managed DDoS Protection service and SDN Managed Firewall service. This report covers SDN services from January 1 – June 30, 2019. It represents a unique view of the cybersecurity trends SDN is seeing in the region. Sign up to receive the report every quarter at **sdncommunications.com/threat-landscape/.**

SDN MANAGED DDoS* PROTECTION: KEY TRENDS January 1 - June 30, 2019

Q1 & Q2 2019 Total Number of Attacks

2124 high alerts

Easily on pace to exceed the total number of attacks reported in 2018 (2759) and we are only halfway through the year.

Attack Count Year over Year

66% increase

Average Duration

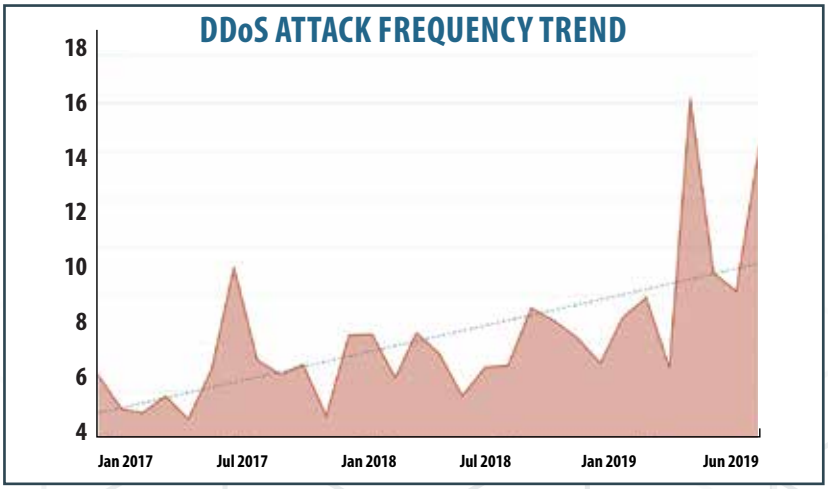
21% decrease

Average Attack Size Change**

38% increase

Peak Attack Size Change**

13% increase



*These results exclude identified tests, global alerts not related to a specific customer objects, and likely false positives where the single attack vector is total traffic.

** Attack size, is determined by total traffic crossing the network directed to an endpoint during detected anomalous activity.

SDN MANAGED DDoS PROTECTION: KEY TRENDS January 1 - June 30, 2019

THREE TYPES OF DDoS ATTACKS

Volumetric Attacks focus entirely on consuming the bandwidth of a network or the connection a network maintains to the rest of the internet. This is the most common type of DDoS attack.

Examples: NTP Amplification, DNS Amplification, UDP Flood, TCP Flood

Protocol Attacks render a target inaccessible by consuming all the resources available on a server or the resources on the intermediate communication equipment, such as firewalls and load balancers.

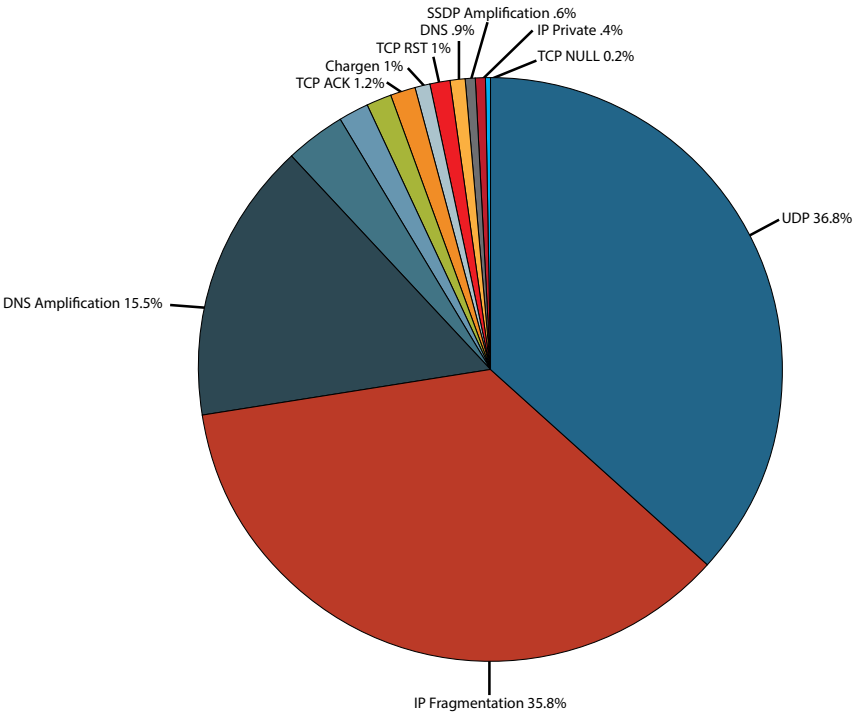
Examples: Syn Flood, Ping of Death

Application-Layer Attacks target a specific weakness found in an application or service at Layer 7. These attacks are the most effective due to taking the "low and slow" approach and circumventing flow-based monitoring solutions.

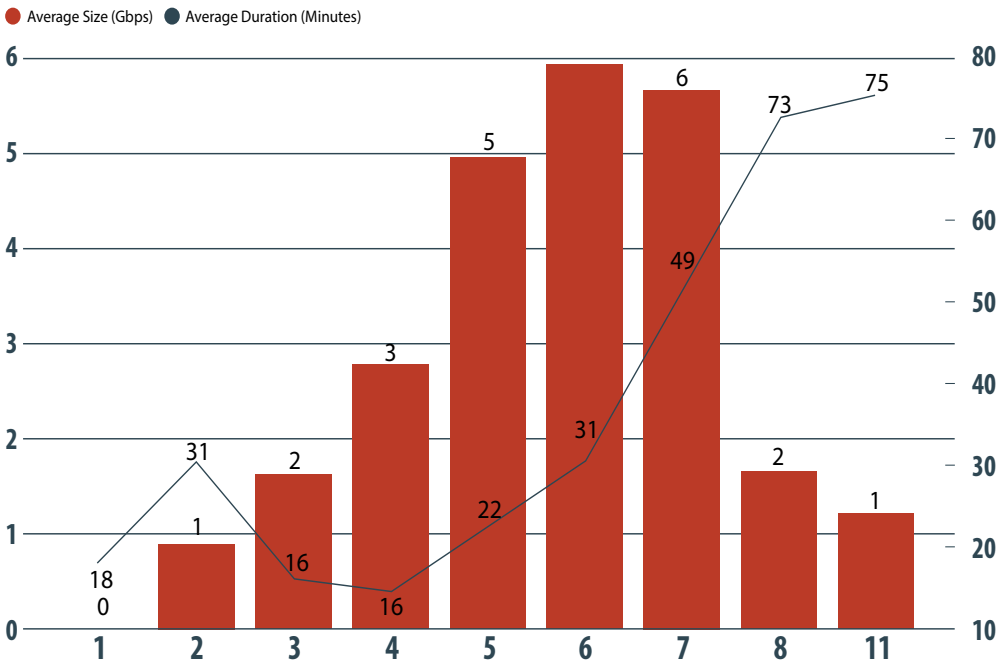
Examples: HTTP Flood, Attack on DNS Services

85% of all DDoS attacks in the first half of 2019 were multi-vector attacks.

2019 Q1 & Q2 ATTACKS BY VECTOR



AVERAGE ATTACK SIZE BY NUMBER OF VECTORS



Seven vectors of attack remains the "sweet spot" as it was in Q1-Q2 of 2018. But the average size of a 7-vector attack jumped from 5.59 Gbps to 22.01 (293.73% increase)

SDN MANAGED FIREWALL: KEY TRENDS January 1 - June 30, 2019

TOP 10 ATTACKS

#1 OpenVAS.Web.Scanner	Port scan attack
#2 PHP.Diescan	Information disclosure
#3 NETGEAR.WNR2000v5.Unauthenticated.Hidden.avi.Stack.Overflow	Remote code execution
#4 HTTP.URI.SQL.Injection	SQL injection
#5 ZmEu.Vulnerability.Scanner	Port scan attack
#6 TCP.Split.Handshake	Information disclosure
#7 Qualys.Vulnerability.Scanner	Port scan attack
#8 Bash.Function.Definitions.Remote.Code.Execution	Remote code execution
#9 WebRTC.Local.IP.Addresses.Disclosure	Information disclosure
#10 ThinkPHP.Controller.Parameter.Remote.Code.Execution	Remote code execution

Scanning attacks have a relatively low severity when compared with other types of attacks since they aren't inherently dangerous to a network. They can be a sign that a more sophisticated attack is being created and tailored to any vulnerabilities found within the port scan.

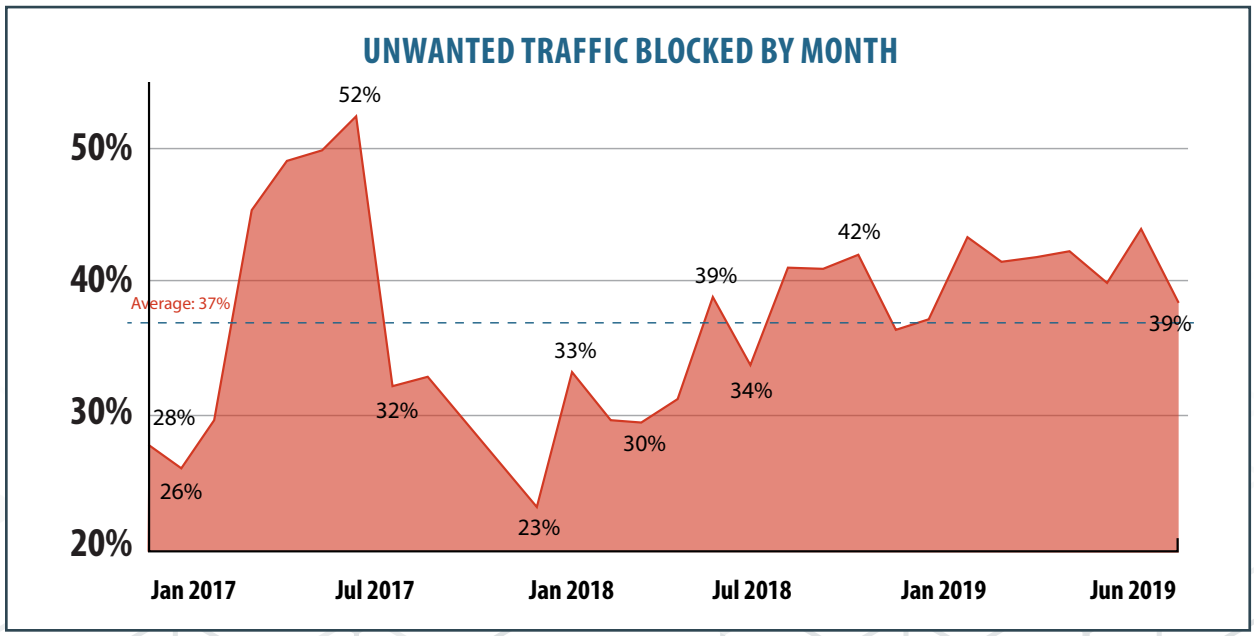
MANAGED FIREWALL PREVENTED

YEAR-OVER-YEAR CHANGE IN BLOCKED TRAFFIC

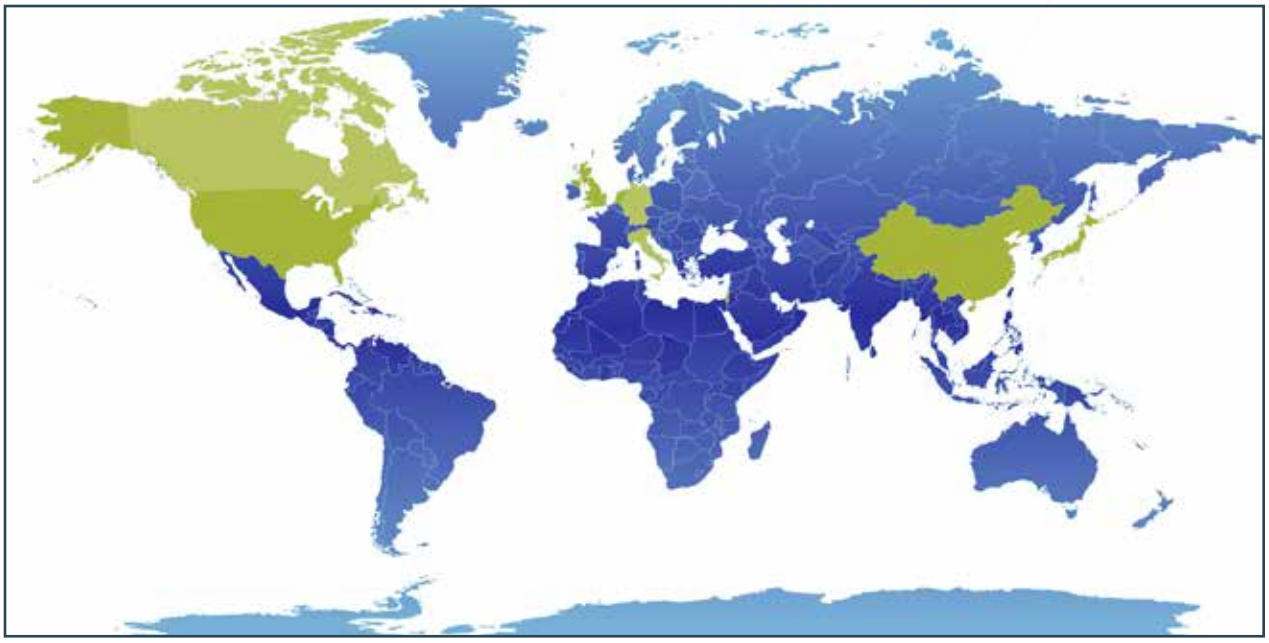
2019 Q1 & Q2	41.04%
2018 Q1 & Q2	32.83%

41.04% OF ALL

SDN Managed Firewall traffic was flagged as malicious or spam and was filtered out.



TOP 10 THREAT EVENTS BY COUNTRY AS SEEN BY SDN MANAGED FIREWALLS



#1 UNITED STATES
#2 CHINA
#3 JAPAN
#4 GERMANY
#5 ITALY
#6 ISRAEL
#7 UNITED KINGDOM
#8 CANADA
#9 NETHERLANDS
#10 HONG KONG

TAKEAWAYS

- Distributed Denial of Service (DDoS) isn't going away as a security concern. In fact, it's a growing issue. While there are fluctuations in size and frequency – overall it continues to grow as an attack medium in size and complexity.
- We are not in a safe corner of our world in the Midwest. We see the same sort of trends in our region as well. Trends at the national and world levels are mirrored in our Managed DDoS protection and Managed Firewall systems as well.

GLOBAL TRENDS FROM NETSCOUT BY ARBOR*

- Geopolitical adversaries increasingly target one another using cyber tactics ranging from malware and DDoS attacks to social engineering and misinformation.
- It can take only five days to go from new attack vector discovery to weaponization, giving anybody with a grudge fast access to inexpensive — and devastatingly effective — tools for revenge.
- In the first half of 2019, DDoS attack frequency grew 39% compared with the first half of 2018. In particular, bad actors feasted on the juicy middle of attack sizes, resulting in staggering growth of 776% in attacks between 100 Gbps and 400 Gbps in size.

* NETSCOUT is powered by Active Threat Level Analysis System (ATLAS®) is a collaborative partnership with more than 330 service provider customers who share anonymous traffic data with Arbor Networks to deliver a comprehensive, aggregated view of global traffic and threats.

SDN COMMUNICATIONS®

www.sdncommunications.com • 2900 W. 10th Street, Sioux Falls, SD 57104 • 1.800.247.1442